- Published version -01 of the draft
- Deployed initial server implementation to Let’s Encrypt’s Staging environment
- Began initial client implementation in Certbot
- renewalInfo URL is now constructable from subscriber certificate
- GET is the only supported protocol (not POST-as-GET)
- Clarified client behavior in various extraordinary circumstances
- Small formatting cleanups
Constructing an ARI URL

- Base path is contained in directory

GET https://example.com/directory

HTTP/1.1 200 OK
Content-Type: application/json

{
  "newNonce": "https://example.com/new-nonce",
  "newAccount": "https://example.com/new-account",
  "newOrder": "https://example.com/new-order",
  "newAuthz": "https://example.com/new-authz",
  "revokeCert": "https://example.com/revoke-cert",
  "keyChange": "https://example.com/key-change",
  "renewalInfo": "https://example.com/renewal-info",
  "meta": {
    "website": "https://www.example.com/",
    "caaaIdentities": ["example.com"],
    "externalAccountRequired": false
  }
}
Constructing an ARI URL

- Remainder is constructed from case-insensitive hex-encodings of:
  - Issuer Key Hash (SHA1)
  - Issuer Name Hash (SHA1)
  - Serial
- These are the same components as OCSP

```plaintext
GET https://example.com/renewal-info
/254581685026383D3B2D2CBECD6AD9B63DB36663
/06FE0BABD8E6746EFCC4730285F7A9487ED1344F
/BCDF4596B6BDC523

HTTP/1.1 200 OK
Content-Type: application/json
Retry-After: "21600"

{
  "suggestedWindow": {
    "start": "2021-01-03T00:00:00Z",
    "end": "2021-01-07T00:00:00Z"
  }
}
```
Open Questions

- **Polling semantics**
  - Retry-After gives half of what we want: “wait X time”
  - But not the other half: “and then query again ASAP”
  - Include polling interval in Directory? Where?
  - Include polling interval in renewalInfo response object?

- **Callback endpoint?**
  - Being notified that renewal has completed would let ACME CA revoke
  - Maybe a POST-as-GET to same renewalInfo URL?

- **Call for adoption**